ABSTRACT OF THE DISCLOSURE

The encryption device includes random number generator means for generating a random number; and a first selector for selecting one of q fixed values in response to the random number, a second selector for selecting one set of q sets of fixed tables in response to the random number. XOR means XORs an input with an XOR of a key with the fixed value. Nonlinear transform means nonlinearly transforms an input in accordance with the selected set of fixed table. Another encryption device includes a plurality of encrypting units coupled in parallel, and a selector for selecting one of the plurality of encrypting units in response to the random number. The masking with the fixed values improves of the processing speed and reduces the required RAM area.